基于 Bell 态纠缠交换的身份认证协议 *

熊金鑫[1]，方　杰[2†]，昌　燕[1]，张仕斌[1]

(1. 成都信息工程大学 信息安全工程学院，成都 610225; 2. 四川省计算机研究院，成都 610041)

摘　要： 提出了一种新的量子身份认证协议，该协议以 Bell 态为传输载体，利用 Bell 态纠缠交换和 Bell 基测量对通信用户进行身份认证。两个 Bell 态的传送过程中不需要做任何的幺正变换，只需要执行 Bell 基测量和按位异或运算就可以实现信息的传输。整个过程中，量子载体操作简单且容易实现。此外，也验证了此协议的正确性。

关键词： 量子身份认证；纠缠交换；Bell 基测量

中图分类号： TP309.2　　doi: 10.3969/j.issn.1001-3695.2017.11.1000

Quantum identity authentication protocol based on Bell states and entanglement swapping

Xiong Jinxin[1], Fang Jie[2†], Chang Yan[1], Zhang Shibin[1]

(1. *School of Cybersecurity*, *Chengdu University of Information Technology*, *Chengdu* 610225, *China*; 2. *Sichuan Institute of Computer Science*, *Chengdu* 610041, *China*)

Abstract: This paper presented a new quantum authentication protocols. The protocol took Bell state as the transmission carrier and used Bell state entanglement swapping and Bell basis measurement to authenticate communication users. There was no need to do any unitary transformation in the transmission of two Bell states. Only need to perform Bell basis measurement and bitwise XOR operation could achieve the transmission of information. Throughout the process, the quantum carrier was simple and easy to implement. In addition, this paper also verified the correctness of this protocol.

Key Words: quantum identity authentication; entanglement swapping; Bell basis measurement

0　引言

自 Bennett 和 Brassard 提出量子密钥分配（QKD）协议（简称 BB84 协议）[1]开辟了量子密码学之后，为了适应各种用途和解决新出现的信息安全问题，研究人员提出了大量的量子密码协议，主要包括量子秘密共享 (quantum secret sharing,QSS)[2,3]、量子安全直接通信(quantum secure direct communication,QSDC[4,5]、量子身份认证(quantum identity authentication, QIA)[6~13]等方面的研究。

量子通信是量子领域中最重要的应用之一，近年来已经在理论和实验上都不断取得突破和进展。但是在量子通信网络中，难免会存在非法用户冒充合法用户，破坏量子通信系统的安全性。在量子通信中存在这样的一个情况，一个假冒合法用户的恶意攻击者可以与其他用户分发密钥且进行秘密通信，即发送伪造的信息给合法用户或者窃取合法用户的秘密信息。同时在量子密钥分配协议中,需要在通信双方建立抗干扰信道或者用经典的方法来相互认证身份。在通信中抗干扰信道很难实现，并且经典身份认证协议又很难达到无条件安全。量子密钥分配协议中难于有效地防止冒充攻击。尤其在攻击者对通信双方的量子信道和经典通信信道在一定的技术条件下,通信过程中遭受中间攻击者的概率大大增加。因此，本协议在量子密钥分配协议中或量子安全直接通信中对用户双方做量子身份认证，从而避免量子安全通信的中间人的攻击，也不需要在量子密钥分配的通信信道建立抗干扰信道和采用经典身份认证。这样的设计同样可以应用在身份识别的智能卡系统之中[12,13]。不同的智能卡拥有不同的 ID，根据不同 ID 制备不同的 Bell 态粒子，采用量子身份认证的方式来完成智能卡的身份认证。用量子的测不准定理和量子不可克隆定理保证了认证的无条件安全。近些年，量子身份认证作为量子密码学比较热门的分支走入研究者的视野，并得到了研究者的广泛关注和深入研究。

目前量子身份认证方案有以下几类：第一类为点对点的量子身份认证方案。2014 年 Yuan 等人[6]提出了一种基于乒乓技

基金项目： 国家自然科学基金资助项目(61572086,61402058)；四川省科技计划项目(20717YY168)；国家重点研究发展计划资助项目(2017YFB0802302)；四川量子安全通信创新团队项目（17TD0009）；四川省学术和技术领导人培训资金支持项目（2016120080102643）；成都信息工程大学中青年学术研究基金资助项目（J201511）

作者简介： 熊金鑫（1990-），男，河南信阳人，硕士研究生，主要研究方向为量子安全通信；方杰（1981-），男（通信作者），四川雅安人，工程师，硕士，主要研究方向为计算机应用技术（816983@qq.com）；昌燕（1979-），女（蒙古族），内蒙古人，副教授，工学博士，主要研究方向为量子密码、信息安全；张仕斌（1971-），男，重庆丰都人，教授，工学博士，主要研究方向为量子安全通信、网络空间安全.

术的无纠缠的单粒子量子身份认证方案。2016 年 Ma 等人[7]采用双模压缩真空态和相干态，提出一种基于量子隐形传态的连续变量量子身份认证协议，该协议用新定义的保真度参数有效地验证用户的身份。第二类是身份认证和量子密钥分配相结合，在传输密钥的同时实现身份认证。2017 年 Ma 等人[8]提出了一种基于独立于测量设备的量子密钥分配（MDI-QKD）协议的新型双向身份认证方案,该协议利用 Bell 态为载体在一轮中实现身份认证和密钥分发。第三类为网络中的量子身份认证方案。Yang 等人[9]提出一个基于 GHZ 态的多方量子身份认证协议，多用户可以由可信第三方同时认证。2013 年 Yang 等人[10]再次提出了一种基于 GHZ 态的(t,n)门限的多方身份认证方案。2014 年张沛等人[11]提出了基于量子隐形传态的无线通信网络身份认证方案。

本文提出了一个基于 Bell 态纠缠交换的身份认证协议。在该协议中两个用户只需要根据用户二进制身份字符串进行 Bell 态的制备、粒子交换、Bell 基测量和进行按位异或运算，就可以实现对通信双方身份的认证。因此与 Ma 等人[7]提出的基于量子隐形传态的连续变量量子身份认证协议相比，虽然在身份认证中不能实现密钥的更新，但协议不需要第三方的介入和定义参数，减少了认证协议的复杂度。与 Ma 等人[8]提出的基于独立于测量设备的量子密钥分配协议的身份认证方案相比，本文协议不需要复杂的量子操控技术，降低了系统执行所需要的条件，提高了协议的实用性。且本文协议在目前的实际技术条件下是容易实现的。

1 准备知识

四个 Bell 态可以表示如下

$$\left|\phi^{\pm}\right\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle \pm|11\rangle\right),\left|\psi^{\pm}\right\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle \pm|10\rangle\right) \tag{1}$$

如果有两个 Bell 态都处于$\left|\phi^{+}\right\rangle$态，则有下面的等式成立：

$$\begin{aligned}\left|\phi^{+}\right\rangle_{12}\left|\phi^{+}\right\rangle_{34}&=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{12}\otimes\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{34}\\&=\frac{1}{2}\begin{pmatrix}\left|\phi^{+}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}+\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}\\+\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}+\left|\psi^{-}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}\end{pmatrix}\end{aligned} \tag{2}$$

如果对粒子 1、3 进行 Bell 基测量，粒子 2、4 就会纠缠在一起。例如，如果对粒子 1、3 测量结果为$\left|\phi^{+}\right\rangle_{13}$（$\left|\phi^{-}\right\rangle_{13}$，$\left|\psi^{+}\right\rangle_{13}$或$\left|\psi^{-}\right\rangle_{13}$），那么对应粒子 2、4 的状态为$\left|\phi^{+}\right\rangle_{24}$（$\left|\varphi^{-}\right\rangle_{24}$，$\left|\psi^{+}\right\rangle_{24}$或$\left|\psi^{-}\right\rangle_{24}$）。

根据这个等式，很容易推导出任意两个 Bell 态经过纠缠交换都以 1/4 的概率的处于四种 Bell 态。如果不考虑其相位，任意两个 Bell 态的纠缠交换情况如表 1 所示。

表 1 任意两个 Bell 态的纠缠交换

Bell 态	Bell 态	纠缠交换两个 Bell 态
$\left\|\varphi^{+}\right\rangle_{12}$	$\left\|\varphi^{+}\right\rangle_{34}$	$\left\|\varphi^{+}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$
$\left\|\varphi^{+}\right\rangle_{12}$	$\left\|\varphi^{-}\right\rangle_{34}$	$\left\|\varphi^{+}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$
$\left\|\varphi^{+}\right\rangle_{12}$	$\left\|\psi^{+}\right\rangle_{34}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24}$
$\left\|\varphi^{+}\right\rangle_{12}$	$\left\|\psi^{-}\right\rangle_{34}$	$\left\|\varphi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24}$
$\left\|\varphi^{-}\right\rangle_{12}$	$\left\|\varphi^{+}\right\rangle_{34}$	$\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$
$\left\|\varphi^{-}\right\rangle_{12}$	$\left\|\varphi^{-}\right\rangle_{34}$	$\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$
$\left\|\varphi^{-}\right\rangle_{12}$	$\left\|\psi^{+}\right\rangle_{34}$	$\left\|\varphi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24}$
$\left\|\varphi^{-}\right\rangle_{12}$	$\left\|\psi^{-}\right\rangle_{34}$	$\left\|\varphi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24}$
$\left\|\psi^{+}\right\rangle_{12}$	$\left\|\varphi^{+}\right\rangle_{34}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24}$
$\left\|\psi^{+}\right\rangle_{12}$	$\left\|\varphi^{-}\right\rangle_{34}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24}$
$\left\|\psi^{+}\right\rangle_{12}$	$\left\|\psi^{+}\right\rangle_{34}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$
$\left\|\psi^{+}\right\rangle_{12}$	$\left\|\psi^{-}\right\rangle_{34}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24}$
$\left\|\psi^{-}\right\rangle_{12}$	$\left\|\varphi^{+}\right\rangle_{34}$	$\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24}$
$\left\|\psi^{-}\right\rangle_{12}$	$\left\|\varphi^{-}\right\rangle_{34}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24}$
$\left\|\psi^{-}\right\rangle_{12}$	$\left\|\psi^{+}\right\rangle_{34}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24}$
$\left\|\psi^{-}\right\rangle_{12}$	$\left\|\psi^{-}\right\rangle_{34}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24},\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24},\left\|\varphi^{+}\right\rangle_{13}\left\|\varphi^{+}\right\rangle_{24},\left\|\varphi^{-}\right\rangle_{13}\left\|\varphi^{-}\right\rangle_{24}$

如果用 00 来表示$\left|\phi^{+}\right\rangle$，01 表示$\left|\phi^{-}\right\rangle$，10 表示$\left|\psi^{+}\right\rangle$，11 表示$\left|\psi^{-}\right\rangle$，那么纠缠交换前两个 Bell 态的二进制表示分别为c_{12}和c_{34}，纠缠交换后的两个 Bell 态粒子的二进制表示分别为c_{13}和c_{24}。由表 1 可以得出，纠缠交换后的两个 Bell 态分别以 1/4 的概率处于$\left|\phi^{+}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}$,以 1/4 的概率处于$\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}$,以 1/4 的概率处于$\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}$,以 1/4 的概率处于$\left|\psi^{-}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}$。如果纠缠交换后的两个 Bell 态为$\left|\phi^{+}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}$，那么有$c_{13}\oplus c_{24}=00\oplus 00=00$，其中$\oplus$表示按位异或操作；如果纠缠交换后的两个 Bell 态为$\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}$，那么有$c_{13}\oplus c_{24}=01\oplus 01=00$；如果纠缠交换后的两个 Bell 态为$\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}$，那么有$c_{13}\oplus c_{24}=10\oplus 10=00$；如果纠缠交换后的两个 Bell 态为$\left|\psi^{-}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}$，那么有$c_{13}\oplus c_{24}=11\oplus 11=00$。由此可得到$c_{12}\oplus c_{34}$的结果等于$c_{13}\oplus c_{24}$的结果。关系如式(3)所示。经推导，任意两个 Bell 态都存在式(3)这个关系。

$$c_{12}\oplus c_{34}=c_{13}\oplus c_{24} \tag{3}$$

任意两个 Bell 态纠缠交换对应的二进制关系如表 2 所示。

假设$ID_A=\{C_{12}^1,C_{12}^2,\ldots\ldots,C_{12}^{2n}\}$是 Alice 的二进制身份字符串，$ID_B=\{C_{34}^1,C_{34}^2,\ldots\ldots,C_{34}^{2n}\}$是 Bob 的二进制身份字符串。Alice 和 Bob 共享ID_A和ID_B。Alice 根据ID_A制备粒子序列S_{ID_A}，Bob 根

据 ID_B 制备粒子序列 S_{ID_B}。制备的规则是：如果身份字符串的当前位为00制备粒子处于 $|\phi^+\rangle$，当前位为01制备粒子处于 $|\phi^-\rangle$，当前位为 10 制备 $|\psi^+\rangle$，当前位为 11 制备 $|\psi^-\rangle$。Alice 把 S_{ID_A} 所有 Bell 态的第一个粒子发送给 Bob，同时 Bob 把 S_{ID_B} 所有 Bell 态的第二个粒子发送给 Alice。Alice 对手中粒子进行 Bell 基测量，此时 Bob 手中粒子对应处于纠缠态。纠缠交换后 Alice 拥有粒子序列 S_{ID_A}'，Bob 拥有粒子序列 S_{ID_B}'。S_{ID_A}' 的二进制表示为 $C_{ID_A}'=\left\{C_{13}^1,C_{13}^2,\ldots\ldots,C_{13}^{2n}\right\}$，$S_{ID_B}'$ 的二进制表示为 $C_{ID_B}'=\left\{C_{24}^1,C_{24}^2,\ldots\ldots,C_{24}^{2n}\right\}$。由 $C_{12}^k\oplus C_{34}^k=C_{13}^k\oplus C_{24}^k(k\in N^*)$ 得到：

$$ID_A\oplus ID_B=C_{ID_A}'\oplus C_{ID_B}' \tag{4}$$

表 2　两个 Bell 态纠缠交换二进制关系

c_{12}	c_{34}	纠缠交换后 $c_{13}\oplus c_{24}$
00	00	00 ⊕ 00=00,01 ⊕ 01=00, 10 ⊕ 10=00,11 ⊕ 11=00
00	01	00 ⊕ 01=01,01 ⊕ 00=01, 10 ⊕ 11=01,11 ⊕ 10=01
00	10	00 ⊕ 10=10,10 ⊕ 00=10, 01 ⊕ 11=10,11 ⊕ 01=10
00	11	00 ⊕ 11=11,11 ⊕ 00=11, 01 ⊕ 10=11,10 ⊕ 01=11
01	00	01 ⊕ 00=01,00 ⊕ 01=01, 10 ⊕ 11=01,11 ⊕ 10=01
01	01	01 ⊕ 01=00,00 ⊕ 00=00, 10 ⊕ 10=00,11 ⊕ 11=00
01	10	01 ⊕ 10=11,10 ⊕ 01=11, 00 ⊕ 11=11,11 ⊕ 00=11
01	11	01 ⊕ 11=10,11 ⊕ 01=10, 00 ⊕ 10=10,10 ⊕ 00=10
10	00	10 ⊕ 00=10,00 ⊕ 10=10, 01 ⊕ 11=10,11 ⊕ 01=10
10	01	10 ⊕ 01=11,01 ⊕ 10=11, 00 ⊕ 11=11,11 ⊕ 00=11
10	10	10 ⊕ 10=00,00 ⊕ 00=00, 01 ⊕ 01=00,10 ⊕ 10=00
10	11	10 ⊕ 11=01,11 ⊕ 10=01, 00 ⊕ 01=01,01 ⊕ 00=01
11	00	11 ⊕ 00=11,00 ⊕ 11=11, 01 ⊕ 10=11,10 ⊕ 01=11
11	01	11 ⊕ 01=10,01 ⊕ 11=10, 00 ⊕ 10=10,10 ⊕ 00=10
11	10	11 ⊕ 10=01,10 ⊕ 11=01, 01 ⊕ 00=01,00 ⊕ 01=01
11	11	11 ⊕ 11=00,10 ⊕ 10=00, 00 ⊕ 00=00,01 ⊕ 01=00

若 Alice 对 Bob 进行身份认证，只需要通过经典信道通知 Bob 公布 C_{ID_B}'。Alice 计算 $ID_A\oplus ID_B=C_{ID_A}'\oplus C_{ID_B}'$ 进行验证，若符合该公式，则证明 Bob 是合法用户。同理，若 Bob 对 Alice 进行身份认证，重新按照规则制备粒子，完成粒子交换等过程后，通过经典信道通知 Alice 公布 C_{ID_A}' 即可。该方式实现了身份认证的功能，并且一方用户公布 C_{ID_A}' 或 C_{ID_B}'，不会引起双方身份信息的泄露。

2　身份认证协议

2.1　协议内容

a)Alice 的二进制串身份字符串为 $ID_A=\{C_{12}^1,C_{12}^2,\ldots\ldots,C_{12}^{2n}\}$，Bob 的二进制身份字符串为 $ID_B=\{C_{34}^1,C_{34}^2,\ldots\ldots,C_{34}^{2n}\}$。Alice 和 Bob 共享 ID_A 和 ID_B。

b)Alice 根据 ID_A 制备粒子序列 S_{ID_A}，Bob 根据 ID_B 制备粒子序列 S_{ID_B}。制备的规则是：如果身份字符串的当前位为 00 制备粒子处于 $|\varphi^+\rangle$，当前位为 01 制备粒子处于 $|\varphi^-\rangle$，当前位为 10 制备 $|\psi^+\rangle$，当前位为 11 制备 $|\psi^-\rangle$。

c)Alice 把 S_{ID_A} 所有 Bell 态的第二个粒子发送给 Bob，同时 Bob 把 S_{ID_B} 所有 Bell 态的第一个粒子发送给 Alice。粒子交换后 Alice 拥有粒子序列 S_{ID_A}'，Bob 拥有粒子序列 S_{ID_B}'。Alice 对 S_{ID_A}' 进行 Bell 基测量，此时 S_{ID_B}' 对应处于纠缠态，Bob 对 S_{ID_B}' 进行 Bell 基测量，此时完成纠缠交换。

d)测量结果进行二进制位表示。表示规则为：用 00 来表示 $|\phi^+\rangle$，01 表示 $|\phi^-\rangle$，10 表示 $|\psi^+\rangle$，11 表示 $|\psi^-\rangle$。S_{ID_A}' 的二进制表示为 C_{ID_A}'，S_{ID_B}' 的二进制表示为 C_{ID_B}'

e)假如 Alice 对 Bob 进行身份认证，只需要通过经典信道通知 Bob 公布 C_{ID_B}'，然后根据式（4）进行验证。若符合该公式，则证明是合法者。若 Bob 对 Alice 进行身份认证，需要重新经过步骤 a)~d)，Bob 通过经典信道通知 Alice 公布 C_{ID_A}'，符合式（4）则证明是合法者。

身份认证过程如图 1 所示。

图 1 显示了该协议身份认证过程。

2.2　协议举例

a)Alice 的二进制串身份字符串为 ID_A=11110100，Bob 的二进制身份字符串为 ID_B=11100010。Alice 和 Bob 共享 ID_A 和 ID_B。

b)Alice 根据 ID_A 制备粒子序列 $S_{ID_A}=\{|\psi^-\rangle,|\psi^-\rangle,|\varphi^-\rangle,|\varphi^+\rangle\}$，Bob 根据 ID_B 制备粒子序列 $S_{ID_B}=\{|\psi^-\rangle,|\psi^+\rangle,|\varphi^+\rangle,|\psi^+\rangle\}$。制备的规则是：如果身份字符串的当前位为 00 制备粒子处于 $|\phi^+\rangle$，当前位为 01 制备粒子处于 $|\phi^-\rangle$，当前位为 10 制备 $|\psi^+\rangle$，当前位为 11 制备 $|\psi^-\rangle$。

c)Alice 把 S_{ID_A} 所有 Bell 态的第一个粒子发送给 Bob，同时 Bob 把 S_{ID_B} 所有 Bell 态的第二个粒子发送给 Alice。粒子交换后 Alice 拥有粒子序列 S_{ID_A}'，Bob 拥有粒子序列 S_{ID_B}'。Alice 对 S_{ID_A}' 进行 Bell 基测量，此时 S_{ID_B}' 对应处于纠缠态，Bob 对 S_{ID_B}' 进行 Bell 基测量，此时完成纠缠交换。Alice 拥有粒子序列 $S_{ID_A}'=\left\{|\psi^-\rangle,|\psi^+\rangle,|\varphi^+\rangle,|\psi^+\rangle\right\}$，Bob 拥有粒子序列 $S_{ID_B}'=\left\{|\psi^-\rangle,|\psi^-\rangle,|\phi^-\rangle,|\phi^+\rangle\right\}$。

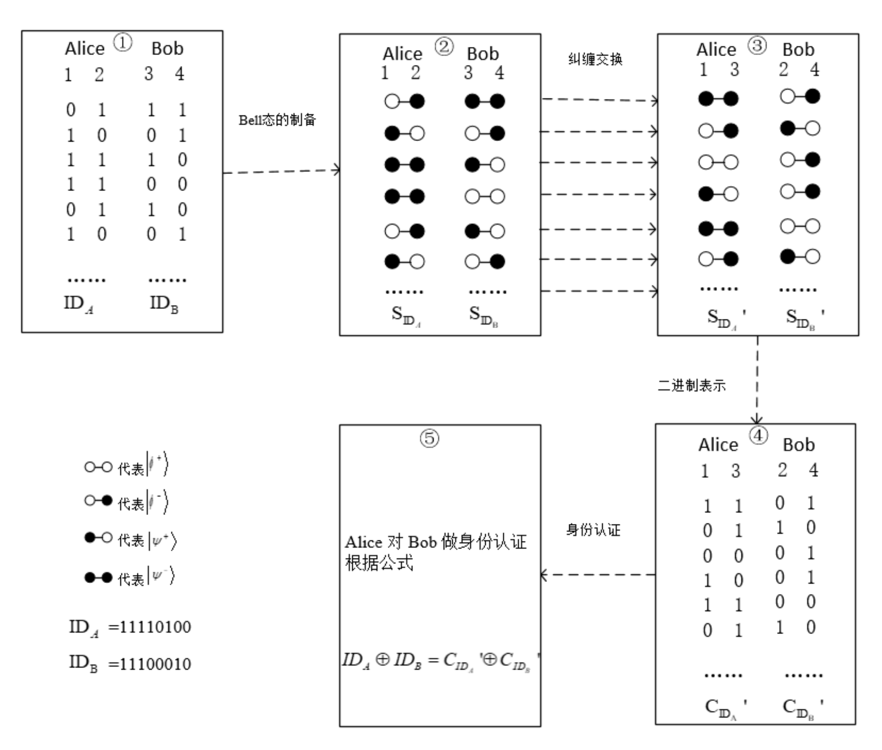


图 1　身份认证过程

d)测量结果进行二进制位表示。表示规则为：用 00 来表示 $|\phi^+\rangle$，01 表示 $|\phi^-\rangle$，10 表示 $|\psi^+\rangle$，11 表示 $|\psi^-\rangle$。S_{ID_A}' 的二进制表示为 C_{ID_A}' =11100010，S_{ID_B}' 的二进制表示为 C_{ID_B}' =11110100。

e)假如 Alice 对 Bob 进行身份认证。只需要通过经典信道通知 Bob 公布 C_{ID_B}'。根据式（4）验证，$11110100 \oplus 11100010=11100010 \oplus 11110100=00010110$。符合该公式，证明 Bob 是合法者。若 Bob 对 Alice 进行身份认证，需要重新经过步骤 a)~d)，Bob 通过经典信道通知 Alice 公布 C_{ID_A}'，符合式（4）则证明是合法者。

3　安全性分析

本文提出的身份认证即可防止非法用户冒充合法用户，又可以保证 ID_A 和 ID_B 的安全性。

3.1　冒充攻击

Eve 在不知道 ID_B 的情况下冒充 Bob 进行通信。由于 Eve 不知道 ID_B，Eve 随机制备 Bell 态粒子序列 S_{ID_E}。Alice 把 S_{ID_A} 所有 Bell 态的第一个粒子发送给 Bob，同时 Eve 把 S_{ID_E} 所有 Bell 态的第一个粒子发送给 Alice。粒子交换后，Alice 拥有粒子序列 S_{ID_A}'，Eve 拥有粒子序列 S_{ID_E}'。Alice 对 S_{ID_A}' 进行 Bell 基测量，同时 Eve 对 S_{ID_E}' 进行 Bell 基测量，此时完成纠缠交换。随后，Alice 对测量结果进行二进制表示为 C_{ID_A}'，Eve 对测量结果进行二进制表示为 C_{ID_E}'。假如 Alice 对 bob 进行身份认证，此时 Eve 公布 C_{ID_E}'，Alice 根据式(4)进行验证，由于 $ID_A \oplus ID_B \neq C_{ID_A}' \oplus C_{ID_E}'$，Eve 不能通过身份认证。所以 Eve 在不知道 ID_B 的情况下，冒充 Bob 不会通过身份认证。同理 Eve 冒充 Alice 也不能通过身份认证。

Eve 可以尝试截取/重发进而推测出 C_{ID_B}'。若 Eve 截获了者 Bob 传送的粒子，使得 S_{ID_A}' 和 S_{ID_B}' 不能够完成纠缠交换。在 Alice 和 Bob 进行身份认证时导致式(4)无法成立，身份认证不能通过。

3.2　ID_A 和 ID_B 的安全性

因为 ID_A 和 ID_B 是通信双方在通信之前事先秘密共享的，非法用户不知道 ID_A 和 ID_B。假如 Eve 想要猜出 ID_A 或 ID_B。设 ID_A 和 ID_B 为 2n 位的二进制串。Eve 正确猜出的概率为 $1/4^n$。只要设定的 ID_A 或 ID_B 的位数足够长，Eve 猜对 ID_A 或 ID_B 的概率将趋近于零。这样以来 Eve 也根本无法通过身份认证。

Eve 尝试采取截获/重发攻击来得到 ID_A 或 ID_B。Eve 截取 Alice 发送的粒子，用 Z 基测量，Eve 依然无法推断出 Alice 制备的粒子序列。而且由于 Eve 的测量会造成 Alice 手中粒子的塌缩，使得 Alice 和 Bob 制备的两组 Bell 态粒子序列无法完成纠缠交换。在 Alice 和 Bob 进行身份认证时导致式(4)无法成立，身份认证不能通过。同理，Eve 采取截获/重发攻击不能得到 ID_B，身份认证一样不能通过。

Eve 试图通过公布的 C_{ID_A}' 或 C_{ID_B}' 得到 ID_A 和 ID_B。在步骤 c)中 S_{ID_A}' 和 S_{ID_B}' 都以 1/4 的概率随机的处于四种最大混合态 $\{|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$。步骤 d)中 Alice 和 Bob 分别对 S_{ID_A}' 和 S_{ID_B}' 进行二进制表示为 C_{ID_A}' 和 C_{ID_B}'。在步骤 e)中由于公布的 C_{ID_A}' 和 C_{ID_B}' 都是纠缠交换后四个最大混合态的二进制表示，所以 C_{ID_A}' 和 C_{ID_B}' 都以 1/4 的概率处于 $\{00,01,10,11\}$，与 ID_A 和

$\mathrm{ID_B}$ 没有关系。在身份认证的过程中，Eve 无法通过一方公布的 $C_{ID_A}{}'$ 或 $C_{ID_B}{}'$ 推测出 ID_A 和 $\mathrm{ID_B}$ 的任何信息。因此，在协议的执行过程中，一方公布 $C_{ID_A}{}'$ 或 $C_{ID_B}{}'$ 不会造成 ID_A 和 $\mathrm{ID_B}$ 的泄露，ID_A 和 $\mathrm{ID_B}$ 是可以重复使用的。

4 结束语

本文提出了一个基于 Bell 态纠缠交换的身份认证协议。在该协议中，只需将双方的二进制身份字符串按照指定规则制备两组粒子序列。然后 Alice 发送制备 Bell 态粒子序列的第一个粒子给 Bob，Bob 发送制备 Bell 态粒子序列的第二个粒子给 Alice。双方各自对手中粒子进行 Bell 基测量，最后把测量结果进行二进制表示，Alice 或 Bob 公布对应的二进制就可以完成一方的身份认证。在整个身份认证的过程中，Bell 态的传送过程中不需要做任何幺正变换，只需要执行 Bell 态测量和按位异或运算就可以实现信息的传输。在实际应用中该协议的实现只取决于 Bell 态的准确制备和 Bell 态的可靠测量。最后，对该协议也进行了安全性分析，分析表明本协议能够抵御冒充者攻击。协议的执行过程中一方公布 $C_{ID_A}{}'$ 或 $C_{ID_B}{}'$ 不会造成 ID_A 和 $\mathrm{ID_B}$ 的泄露，ID_A 和 $\mathrm{ID_B}$ 是可以重复使用的。

参考文献：

[1] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing [C]// Proc of IEEE International Conference on Computers Systems and Signal Processing. 1984: 175-179.

[2] Bell B A, Markham D, Herrera-Martí D A, et al. Experimental demonstration of graph-state quantum secret sharing [J]. Nature Communications, 2014, 5: 5480.

[3] Mishra S, Shukla C, Pathak A, et al. An integrated hierarchical dynamic quantum secret sharing protocol [J]. International Journal of Theoretical Physics, 2015, 54 (9): 1-12.

[4] Chang Y, Xu C X, Zhang S B, et al. Quantum secure direct communication and authentication protocol with single photons [J]. Chinese Science Bulletin, 2013, 58 (36): 4571-4576.

[5] Li J, Guo X J, Song D, et al, Improved quantum"ping-pong"protocol based on extended three-particle GHZ state [J] China Communications, 2012, 9 (1): 111-116.

[6] Yuan H, Liu Y M, Pan G Z, et al. Quantum identity authentication based on ping-pong technique without entanglements [J]. Quantum Information Processing, 2014, 13 (11): 2535-2549.

[7] Ma H, Huang P, Bao W, et al. Continuous-variable quantum identity authentication based on quantum teleportation [J]. Quantum Information Processing, 2016, 15 (6): 2605-2620

[8] Ma S Q, Zhu C H, Pei C X. A practical identity authentication scheme for measurement-device-independent quantum key distribution [C]// Proc of Computer, Information and Telecommunication Systems. 2017: 274-278.

[9] Yang Y G, Wen Q Y. Economical multiparty simultaneous quantum identity authentication based on greenberger–horne–zeilinger states [J]. Chinese Physics B, 2009, 18 (8): 3233-3237.

[10] Yang Y G, Wang H Y, Jia X, et al. A quantum protocol for (t, n) -threshold identity authentication based on greenberger-horne-zeilinger states [J]. International Journal of Theoretical Physics, 2013, 52 (2): 524-530.

[11] 张沛，周小清，李智伟．基于量子隐形传态的无线通信网络身份认证方案 [J]．物理学报, 2014, 63 (13): 19-24.

[12] Wang D, He D, Wang P et al. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment [J]. IEEE Trans on Dependable and Secure Computing, 2015, 12 (4): 428-442.

[13] Wang D, Wang P. Two birds with one stone: two-factor authentication with security beyond conventional bound [J]. IEEE Trans on Dependable and Secure Computing, 2016, PP (99): 1-22.